

INTERNATIONAL HELLENIC UNIVERSITY

LL.M IN TRANSNATIONAL AND EUROPEAN COMMERCIAL LAW & ALTERNATIVE DISPUTE
RESOLUTION**“THE BIT COIN PHENOMENON”**

By Sofia Papanikolaou

“So, I think that the internet is going to be one of the major forces for reducing the role of government. The one thing that is missing but will soon be developed is a reliable e-cash, a method when buying in the internet where you can transfer funds from A to B without A knowing B or B knowing A. The way in which I can take a dollar bill and hand it to you and there is no record or where it came from and you may get it without knowing who I am. That kind of thing will develop in the internet and that, will make it even easier for people to use the internet. Of course it has its negative side. It means that the gangsters, the people who are engaged in illegal transactions will also have an easier way to carry on their business.”, Milton Friedman¹, 1999.²

¹ http://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/1976/friedman-bio.html

² <http://www.youtube.com/watch?v=6MnQJFEVY7s>

1. Introduction

In the summer of 2013, James Howells, a British IT worker, threw his old hard drive device into the garbage. On November 2013, Howells devastated realized that he had thrown approximately 9 million dollars in the trash. The device is now buried under a mountain of garbage at a landfill site in Wales. It will be almost impossible to find. The particular hard drive, held a digital store of 7.500 "bitcoins". The IT worker mined the virtual currency four years ago when it was the exclusive domain of tech geeks. Back then bitcoin was worth very little. On November 2013, the crypto currency broke through \$1,200, making the missing hard drive worth around \$9 million.³

One of the fascinating phenomena of the Internet era is an emergence of digital currencies such as BitCoin, LiteCoin, NameCoin, PPCoin, Ripple and Ven to name the most popular ones. A digital currency can be defined as an alternative currency which is exclusively electronic and thus has no physical form. It is also not issued by any specific central bank or government of a specific country and it is thus practically detached from the real economy. Note that a digital and a virtual currency are not synonymous since the virtual currencies are trading currencies in virtual worlds (most frequently in the massive multiplayer online games – MMOGs – such as World of Warcraft or Second Life. Even though the digital currencies are almost isolated from the real economies, their prices (exchange rates) have experienced quite an erratic behavior recently. The *BitCoin* currency – the most popular of the digital currencies – started the year of 2013 at levels of \$13 per a *BitCoin* and rocketed

³ See <http://money.cnn.com/2013/11/29/news/bitcoin-haul-landfill/>

to \$230 on 9 April 2013 potentially creating an absurd profit of almost 1700% in less than four months. Later the same year, the price soared even higher to \$395 on 9 November 2013, which accounts for a profit of approximately 2900% since the beginning of 2013.⁴

Bitcoin is a private digital currency traded online via a peer-to-peer network. Bitcoins are stored as electronic files on a computer's hard drive, and can be accumulated or transferred just like an e-mail. Software algorithms embedded in the online Bitcoin network protect against fraud and ensure that the files are not counterfeited. Bitcoin was designed to operate without the need for intermediaries or any central issuing authority. Bitcoin does not rely on a central bank to issue it, a commercial bank to store it, or a credit card company to transfer it. Instead, users interact with each other directly and anonymously and without third-party intervention.⁵

2. Background

i. The Birth of the Bitcoin

⁴ (*BitCoin* meets *Google Trends* and *Wikipedia*: Quantifying the relationship between phenomena of the Internet era, Ladislav Kristoufek, Scientific Reports, <http://www.nature.com/srep/2013/131204/srep03415/full/srep03415.html>

⁵ REGULATING DIGITAL CURRENCIES: BRINGING BITCOIN WITHIN THE REACH OF THE IMF ,Nicholas A. Plassaras

“Bitcoin is two things which share a name: 1) a payment system and 2) a currency. You use the Bitcoin system to send bitcoins as currency from one account holder to another.” “Bitcoin is an experimental new digital currency that enables instant payments to anyone, anywhere in the world.” The concept behind Bitcoins began in a 1998 paper by Wei Dai, which circulated in the cypherpunks mailing list. Entitled “b-money, a scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help,” the paper proposed a protocol in which “anyone can create money by broadcasting the solution to a previously unsolved computational problem . . . [from which] it must be easy to determine how much computing effort it took to solve the problem and the solution must otherwise have no value, either practical or intellectual.” Wei Dai’s paper also set forth the idea that “every participant maintains a (separate) database of how much money belongs to each pseudonym” so that, when money is transferred, a message is broadcasted to the database, which records debits and credits of each pseudonym.

Electronic Cash System, created a construct to implement Dai’s theory. Demonstrating an “electronic payment system based on cryptographic proof instead of trust, [Bitcoins] allow[] any two willing parties to transact directly with each other without the need for a trusted third party” such as a financial institution acting as an online payment processor.⁶

⁶ TRUST, IDENTITY, AND DISCLOSURE: ARE BITCOIN EXCHANGES THE NEXT VIRTUAL HAVENS FOR MONEY LAUNDERING AND TAX EVASION?, *Sarah Gruber*

Satoshi Nakamoto in his "A Peer to Peer Electronic cash system states:

"Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need.

A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the

chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.”⁷

ii. Technical nature of the Bitcoin

a. Technical aspects

The technical aspects of this system are complex and not easy to understand without a sound technical background. Therefore, a comprehensive explanation of the underlying technical mechanism of Bitcoin lies outside the scope of this paper. According to the founder, Nakamoto (2009), an electronic coin can be defined as a chain of digital signatures. Each owner of the currency has a pair of keys, one public and one private. These keys are saved locally in a file and, consequently, a loss or deletion of the file would mean that all Bitcoins associated with it are lost as well.⁸

⁷ (satoshi nakamoto “a peer to peer electronic cash system” <http://bitcoin.org/bitcoin.pdf>)

⁸ <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

Once the user has installed a Bitcoin wallet on the computer or mobile phone, it will generate the first Bitcoin address. The block chain is a **shared public ledger** on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography. Cryptography is the branch of mathematics that creates **mathematical proofs that provide high levels of security**. Online commerce and banking already uses cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the block chain. It can also be used to encrypt a wallet, so that it cannot be used without a password.

A transaction is a **transfer of value between Bitcoin wallets** that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. A private key is a **secret piece of data that proves your right to spend bitcoins from a specific wallet** through a cryptographic signature. The private key(s) are stored in the computer in case of a software wallet; they are stored on some remote servers in case of a web wallet. The signature also prevents the transaction from being altered by anybody once it has been issued. A cryptographic signature is a **mathematical mechanism that allows someone to prove ownership**. In the case of Bitcoin, a Bitcoin wallet and its private key(s) are linked by algorithms. When the Bitcoin software signs a transaction

with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. All transactions are broadcast between users and usually begin to be confirmed by the network in the following 10 minutes, through a process called mining. Bitcoin mining is the process of **making computer hardware perform mathematical calculations for the Bitcoin network to confirm transactions** and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done.

Mining is a **distributed consensus system** that is used to confirm waiting transactions by including them in the block chain. Confirmation means that a transaction has been **processed by the network and is highly unlikely to be reversed**. Transactions receive a confirmation when they are included in a block and for each subsequent block. Each confirmation *exponentially* decreases the risk of a reversed transaction. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. A block is a **record in the block chain that contains and confirms many waiting transactions**. Roughly every 10 minutes, on average, a new block including transactions is appended to the block chain through mining. The block chain is a **public record of Bitcoin transactions** in chronological order. The block chain is shared

between all Bitcoin users. It is used to verify the permanence of Bitcoin transactions and to prevent double spending. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the block chain. This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends⁹. “Mining” is therefore the process of validating transactions by using computing power to find valid blocks (i.e. to solve complicated mathematical problems) and is the only way to create new money in the Bitcoin scheme.

According to Nakamoto (2009), mining is also a very reliable procedure for the security and safety of the system as it provides the incentive to act honestly: “if a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or by using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth”. However, as will be explained later, fraudsters may still have non-financial incentives to compromise the system.

Users have several incentives to use Bitcoins. Firstly,

⁹ <http://bitcoin.org/en/how-it-works>

transactions are anonymous, as accounts are not registered and Bitcoins are sent directly from one computer to another. Also, users have the possibility of generating multiple Bitcoin addresses to differentiate or isolate transactions. Secondly, transactions are carried out faster and more cheaply than with traditional means of payment. Transactions fees, if any, are very low and no bank account fee is charged.¹⁰

b. Monetary aspects

Satoshi Nakamoto in his "A peer to peer Electronic cash system" states "By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."

¹⁰ <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

The Bitcoin scheme is designed as a decentralized system where no central monetary authority is involved. Bitcoins can be bought on different platforms. However, new money is created and introduced into the system only via the above-mentioned mining activity, i.e. by rewarding the “miners” who perform the crucial role of validating all transactions made, with new Bitcoins.

Therefore, the supply of money does not depend on the monetary policy of any virtual central bank, but rather evolves based on interested users performing a specific activity. According to Bitcoin, the scheme has been technically designed in such a way that the money supply will develop at a predictable pace .

The algorithms to be solved (i.e. the new blocks to be discovered) in order to receive newly created Bitcoins become more and more complex (more computing resources are needed). As explained on its website, the rate of block creation is approximately constant over time: six per hour, one every ten minutes. However, the number of Bitcoins generated per block is set to decrease geometrically, with a 50% reduction every four years. The result is

that the number of Bitcoins in existence will reach 21 million in around 2040. From this point onwards, miners are expected to finance themselves via transaction fees. In fact, this kind of fee can already be charged by a miner when creating a block.

The fact that the supply of money is clearly determined implies that, in theory, the issuance of money cannot be altered by any central authority or participant wanting to “print” extra money. According to Bitcoin supporters, the system is supposed to avoid inflation, as well as the business cycles originating from extensive money creation. However, the system has been accused of leading to a deflationary spiral. The total supply of Bitcoins is expected to grow geometrically until it reaches a finite limit of 21 million. If, however, the number of Bitcoin users starts growing exponentially for any reason, and assuming that the velocity of money does not increase proportionally, a long-term appreciation of the currency can be expected or, in other words, a depreciation of the prices of the goods and services quoted in Bitcoins. People would have a great incentive to hold Bitcoins and delay their consumption, thereby exacerbating the deflationary spiral. The extent to which this could be a problem in reality is not clear. Two remarks should be made. Firstly, as highlighted by the Economist (2011a), the deflation hypothesis entails an assumption which is not realistic at this stage, i.e. that many more people will want to receive Bitcoins in return for goods or in exchange for paper money. However, Bitcoin is still quite immature and illiquid (the 6.5 million Bitcoins are shared by 10,000 users) which is a clear disincentive for its use. Secondly, Bitcoin is not the currency of a country or currency area and is therefore not directly linked to the goods and services produced in a specific economy, but

linked to the goods and services provided by merchants who accept Bitcoins. These merchants may also accept another currency (e.g. US dollars) and therefore, the fact that deflation is anticipated could give rise to a situation where merchants adapt the prices of their goods and services in Bitcoins.

All currencies must address the problem of counterfeiting; in the context of digital currencies, it is known as the double-spending problem. Because these coins are essentially nothing more than bits of data, the same coin may be copied and used multiple times. While this is not a problem for other types of computer files, the ability to arbitrarily create and spend the same coin erodes one of the facets that makes money valuable: scarcity. Instead of introducing into the system a trusted intermediary to guarantee that the parties do not attempt to double-spend their coins, Bitcoin solves this problem through the use of its block chain. Because all transactions are broadcast to each node in the network and eventually find their way into this public ledger, each node has incontestable proof of the ownership and transactional history of each Bitcoin. The sheer computational force required to alter the block chain ensures that transactions cannot be undone and that the same coin cannot be spent twice.

Bitcoin also manages to provide a certain degree of privacy to its users. Despite each node's access to the block chain, transactions are kept partially anonymous because only the users' Bitcoin addresses (that is, their public keys) are published within it. As no personally identifying information is tied to this address, viewers are only able to discern that one party sent a certain amount of Bitcoins to another. Functionally, this is similar to the way information is released at stock exchanges: trade sizes and times are

published without revealing the identity of the party buying or selling. Nevertheless, the public nature of the block chain means that transactional anonymity is not foolproof, especially if users fail to take additional precautions to maintain their privacy.

Because the Bitcoin system is able to manage all of these functions itself, it reduces its users' reliance on financial intermediaries. As a result, small value transactions are made possible, and the costs of doing business are reduced. Furthermore, the impossibility of payment reversal, combined with the pseudo anonymous nature of Bitcoin payments, allows users to transact with any merchant they see fit, regardless of the questionable nature of that merchant's business. In addition to reducing its dependency on financial intermediaries, the Bitcoin system also needs no central bank to function. The initial issuance of the currency is accomplished through the process of mining, which rewards the system's early adopters in exchange for their help in securing and supporting the network. The network also addresses the issue of regulating the supply of Bitcoins by setting a cap on the amount of Bitcoins that can ever be created at 21 million. Because miners are compensated for validating blocks, an event calculated to occur roughly once a predictable rate.

This aspect of the Bitcoin system should, *in theory*, keep inflation low and place investment and spending decisions on more solid ground. In fact, as the number of Bitcoins issued begins to decline, their value will grow. Slow and steady deflation like this is normally a destructive force in modern economies, primarily because it is unexpected. Bitcoin, on the other hand, should

not fall victim to this problem, because its users will anticipate the effect.¹¹

In order to serve as an efficient unit of account, a currency must provide an almost intuitive measure of relative worth. Without it, users would have to spend time, money, and resources, to determine what the currency is really worth. Gold, for example, derives its value because of its rarity. Recall that generating a Bitcoin involves an incredibly complex and time-consuming process. A Bitcoin, therefore, could be intrinsically and intuitively valuable given how difficult it is to produce. Also, because Bitcoins will not be produced after 2025, they—like gold—might soon be considered “rare.”

In addition, an effective currency must also be accepted as legitimate by its users. Traditional currencies in democratic societies, for example, derive legitimacy from the fact that a government issues, manages, and guarantees the currency by operation of law. While legitimacy in the eyes of a currency’s users is often obtained by government backing, a government’s susceptibility to interest groups can sometimes harm a currency’s stability more than it helps it.⁸⁴ This suggests that the ideal currency should be viewed as legitimate while not relying on government backing.¹²

iii. Bitcoin in e-commerce.

¹¹ The Nature of the Form : Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System, Joshua J. Doguet, Louisiana Law

¹² REGULATING DIGITAL CURRENCIES: BRINGING BITCOIN WITHIN THE REACH OF THE IMF, Nicholas A. Plassaras

Bitcoins are becoming increasingly prevalent in today's economy, as evidenced by the volume of sales to both online and brick-and-mortar merchants in which the buyer paid in Bitcoins. Bitcoins are now accepted in exchange for gift cards, virtual Master Cards, precious metals, cash, 3D paintings, anonymous offshore hosting services, domain registration, flowers, gun parts, a Hackers Handbook, language learning services, gambling services, lottery tickets, books, outdoor survival gear, computers and laptops, t-shirts, luxury jewelry, cupcakes, Australian beef, beauty products, and even prescription drugs. Websites host maps on which "real world shops" can be located that accept Bitcoins as payment. Even non-merchant individuals posting personal comments in discussion forums commonly post their Bitcoin addresses in the comments they make, hoping that another user will find the individual's comments insightful and wish to donate money to the author. One politician running for re-election accepted Bitcoin donations on his campaign website.

Many service providers accept Bitcoins in exchange for legal services, web development, e-mail hosting, web application security testing, financial services, academic assistance, auction services, piano lessons via Skype, oil changes, Kosher meal delivery, taxi services, or even a stay at a bed and breakfast. Many charitable organizations accept Bitcoin donations. Even the financial services industry now caters to the Bitcoin community, offering loan services, stock exchanges, commodity and futures exchanges, foreign exchange trading, and escrow services in the medium of Bitcoins. One article calls Bitcoin the "Wild West of finance, with a proliferation of websites offering loosely regulated replicas of the services familiar to those in the financial industry." One firm based in Malta offers interests in its hedge fund, though it excludes any entity from the United States from participating because "the U.S. jurisdiction is tricky." The famed Winklevoss twins have proposed an exchange traded trust

fund that would trade baskets of Bitcoins. New uses for Bitcoins arise quite frequently, as do new species of cyber currencies that have tweaked the Bitcoin protocol.¹³

In Bitcoin's short lifespan, it has amassed a base of approximately 10,000 users, including several hundred merchants that currently accept the digital currency as a method of payment. However, the currency has yet to find adoption with any mainstream retailers, such as Amazon.com. Despite the fact that the overwhelming majority of these merchants are small businesses that operate in the technology sector, the goods and services provided by the remainder are incredibly diverse. Indeed, they run the gamut from sellers of clothing, home, and car accessories, to brick-and-mortar establishments, like restaurants, hotels, and travel companies. Three attorneys located in the United States have even offered to provide legal services in exchange for Bitcoins. Furthermore, a handful of organizations (including a few nonprofits) accept donations in Bitcoins; among these is the notorious whistle-blowing website, Wikileaks, and the hacker group Lulz Security. Businesses in the financial sector also make up an important part of the Bitcoin economy. While they range from providers of escrow and online wallet services, to mobile payment systems, perhaps the most crucial of these are Bitcoin exchanges. By matching buyers with sellers, these businesses facilitate the conversion of Bitcoins to (and from) at least two dozen established fiat currencies, such as the dollar, euro, and pound sterling.

For individuals looking to transact in Bitcoins without having to mine for them, these exchanges provide the simplest method of

¹³ TRUST, IDENTITY, AND DISCLOSURE: ARE BITCOIN EXCHANGES THE NEXT VIRTUAL HAVENS FOR MONEY LAUNDERING AND TAX EVASION?, *Sarah Gruber*

obtaining the digital currency and also the easiest way to convert Bitcoins back to other fiat currencies. The number of operating exchanges continues to expand and the volume of transactions that pass through them is fairly substantial. For example, Mt. Gox, one of the more popular exchanges, has moved \$70 million in funds in the last six months alone.¹⁴

3. Legal Status Of the Bitcoin

i. Legal Nature of the Bitcoin

A. Bitcoin and the E.U legal framework

Bitcoin's legal framework within the EU is unclear. On August 2013, Germany's ministry of finance has formally recognized the digital currency Bitcoin as a "unit of account" which can be used for private transactions – meaning that the ministry will now be able to tax users or creators of the four-year-old virtual money.¹⁵

¹⁴ The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System
Joshua J. Doguet Louisiana law review

¹⁵ <http://www.theguardian.com/technology/2013/aug/19/bitcoin-unit-of-account-germany>

The implications of Germany's new designation remain uncertain. In June, the Finance Ministry declared that profits on bitcoin investments are tax free after a year. But now it appears that some transactions involving bitcoins could be taxed after all. A tax advisor told the Berlin-based daily *Die Welt* that VAT would only have to be paid by people who use bitcoins commercially.¹⁶

In the EU, there are some who suggest that Bitcoin could fall under the Electronic Money Directive (2009/110/EC). This Directive uses three criteria to define electronic money: (i) it should be stored electronically; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; and (iii) accepted as a means of payment by undertakings other than the issuer.

Can Bitcoin be considered an electronic money institution? Bitcoin probably complies with the first and the third criteria, but not with the second. Moreover, it is important to consider the conversion into another currency, which was clearly not envisaged in the Directive. In fact, Art. 11 explicitly says that "Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held". This cannot be ensured in a virtual currency scheme like Bitcoin. A last key aspect that should

¹⁶ <http://www.spiegel.de/international/business/germany-declares-bitcoins-to-be-a-unit-of-account-a-917525.html>

be taken into account is The “mining” activity, which leads to money creation without the receipt of funds.

It is difficult to assess how this could be interpreted within the scope of the Directive. Another European law that might have some relevance to virtual currency schemes like Bitcoin is the Payment Services Directive (2007/64/EC). This Directive lays down rules on the execution of payment transactions where the funds are electronic money, yet it does not regulate the issuance of electronic money, nor does it amend the prudential regulation of electronic money institutions as provided for in the Electronic Money Directive. Therefore, the new category of payment service provider it introduces – payment institutions – should not be allowed to issue electronic money. As a consequence, Bitcoin clearly falls outside the scope of the Payment Services Directive.

In the meantime, some initial attempts to define the legal status of Bitcoin are already happening In Europe. The French law courts are looking into the issue after local banks shut down the currency exchange facility for accounts handling the currency, on the presumption that Bitcoin should conform to electronic money regulations. Finally, the issue of Bitcoin’s legal framework has been raised in the European Commission’s Payments Committee.¹⁷

¹⁷ European Central Bank “ Virtual Currency Schemes”, October 2012.

B. The US Legal Framework

When first introduced to Bitcoin, individuals often question its legality. In other words, they wonder if someone may lawfully create a private currency like Bitcoin in the United States. In fact, both digital and tangible private currencies are nothing new, the latter having existed in this country for over two centuries.

Looking at the issue in its entirety requires an analysis of certain provisions of the United States Constitution, in addition to an obscure currency-related law—the Stamp Payments Act of 1862. An ultimate finding of legality should have a positive impact on the demand for Bitcoins because legal uncertainty tends to inhibit economic growth.

The Constitution

The Constitution gives Congress the power “to coin money” and “regulate the value thereof” while also prohibiting the states from doing the same. The Framers’ definition of “money,” though, was limited only to coins. While the document also forbids the states from issuing paper money, it is silent concerning the federal government’s ability to do so. Thus, the Constitution goes no further than establishing Congress’s authority over the money of the United States to the exclusion of the states. That is, it does not prohibit the private issuance of currency in as much as it makes no mention of the subject altogether.

The Stamp Payments Act of 1862

In the latter half of the 19th century, Congress finally addressed the issue of private currency. Its action stemmed from a concern that individuals were hoarding United States coins, because the value of their metal surpassed the face value of the coins. The resulting shortage of coins led the issuance of private bank notes of small denomination. Congress responded with the Stamp Payments Act of 1862, which attempted to combat the problem with criminal sanctions. Though the Act has been amended multiple times over the past 150 years, section two remains substantively the same to this day. It provides that:

“Whoever makes, issues, circulates, or pays out any note, check, memorandum, token, or other obligation for a less sum than \$1, intended to circulate as money or to be received or used in lieu of lawful money of the United States, shall be fined under this title or imprisoned not more than six months, or both.”

While Congress has paid some attention to the Act in the modern era, no published court opinions have interpreted its meaning since 1899. Early case law, though limited, is able to provide at least *some* insight as to its application. In *United States v. Van Auken*, the Supreme Court recognized that in passing the Act, Congress primarily intended it “to prevent competition with the national currency.” Thus, it would not apply to anything with a limited circulation. This determination in *Van Auken*, and in similar cases, rested on the fact that the notes were only redeemable in merchandise and that they did not physically resemble the nation’s official currency.

Modern, paper-based, private currencies such as the Ithaca Hour and BerkShare only circulate within particular communities and are only accepted at certain businesses. Furthermore, their values are tied to the U.S. dollar, and their smallest notes are denominated in values greater than one dollar. As such, they have been able to escape criminal liability under the Act. Bitcoin is not geographically constricted like these currencies.

Its supporters are pushing for it to be a widely accepted medium of exchange on the Internet, an aspect that could lead a court to find that Bitcoins, indeed, “circulate as money.” Furthermore, Bitcoin was designed to be economically superior to government-backed currencies, and those who transact in Bitcoins necessarily do so to the exclusion of the U.S. dollar. In this sense, some may see Bitcoin as competing with the nation’s currency. Finally, because Bitcoin is able to restore the practicality of micropayments, there can be little doubt that it will be used to engage in transactions far below the Act’s one-dollar threshold.

There are many valid counterarguments, however, that Bitcoin would fall outside of the Act’s scope. First, because Bitcoins are primarily intended for Internet transactions, they do not actually compete with the currency of the United States; it may be more accurate to say that digital currencies, like Bitcoin, compete with online payment processors, such as PayPal and Dwolla, and credit cards. Second, unlike the previously mentioned community currencies, Bitcoin’s value is not pegged to the dollar, but is determined by supply and demand. As such, an argument can be made that Bitcoin transactions, no matter how small, are not “for a less sum than \$1,” because Bitcoins are not denominated in dollars.

In evaluating how the Stamp Payments Act could apply to digital currencies in general, scholars have suggested that in order for something to “circulate as money,” it must possess the physical characteristics of money. This argument is supported in the text of the Act, which refers to “any note, check, memorandum, token, or other obligation.” Each of these items is a “physical manifestation of currency.” As a digital currency, Bitcoin is completely intangible, a fact that could exclude it from the Act’s reach.

Perhaps the strongest textual argument is that each of the prohibited items in the list above is an obligation, as is indicated by the final phrase “or other obligation.” Unlike many of the items at issue in the cases interpreting the Act, Bitcoins are not obligations because no “entity has promised to provide something in return for [them].” Thus, even if an argument were made that Bitcoins are “digital tokens,” they would fall outside the list’s range, as they are not obligations.

Finally, because the Act was passed to address a shortage of United States coins, its legislative purpose has long since vanished. Although it was stylistically amended as recently as 1994, Congress did not add “digital currency” or any similar term to the list of proscribed items. Their failure to do so could certainly indicate that they did not intend for the Act to apply to such things. Furthermore, it is not likely that when the Act was originally written, lawmakers could have intended for it to encompass digital currencies, a machination of technology that would not be conceived for over 100 more years. In lieu of the continuing expansion in the number of digital currencies, the Treasury Department has requested that the Act be interpreted narrowly by the Department of Justice; some scholars have even called for its repeal. Regardless of the Act’s continued existence, Bitcoin is unlikely to be challenged by it, as the arguments for bringing Bitcoin within its purview are overwhelmingly outweighed by the arguments against doing so. Indeed, digital currencies have been around in some form or another for over a decade and neither their

creators nor their users have yet to be prosecuted under the Act—nor should they be worried about this possibility. As such, the remainder of this Comment surveys the activities occurring within the Bitcoin economy, with a focus on how regulators should respond to its more “concerning” aspects¹⁸.

On March 18, 2013, The Financial Crimes Enforcement Network ("FinCEN") is issuing this interpretive guidance to clarify the applicability of the regulations implementing the Bank Secrecy Act ("BSA") to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. FinCEN's regulations define currency (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance.

“In contrast to real currency, "virtual" currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This guidance addresses "convertible" virtual currency. This type of virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency.”¹⁹

Finally, On 5 August 2013, the first Court ruling referring to the nature of Bitcoin was held by US Texas Court in SECURITIES AND

¹⁸ Louisiana law review, The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System Joshua J. Doguet.

¹⁹ http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

EXCHANGE COMMISSION VS TRENDON T. SHAVERS and BITCOIN SAVINGS AND
TRUST (CASE NO 4:13-CV-416).

Magistrate Judge Amos L. Mazzant states in his memorandum :

“The term “security” is defined as “any note, stock, treasury stock, security future, security-based swap, bond...[or] investment contract...” 15 U.S.C. § 77b. An investment contract is any contract, transaction, or scheme involving (1) an investment of money, (2) in a common enterprise, (3) with the expectation that profits will be derived from the efforts of the promoter or a third party. SEC v. W.J. Howey & Co., 328 U.S. 293, 298-99 (1946); Long v. Shultz Cattle Co, 881 F.2d 129, 132 (1989). First, the Court must determine whether the BTCST investments constitute an investment of money. It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and as Shavers stated, used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money, and investors wishing to invest in BTCST provided an investment of money.”²⁰

²⁰ <http://ia600904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf>

ii. Illegal Activities

The lack of border restrictions, the irreversibility of transactions, and the purposeful removal of government oversight makes Bitcoin, unsurprisingly, a nexus of criminal activity. A significant chunk of Bitcoin transactions occur on the Silk Road, a hidden online marketplace for drugs, which accepts only Bitcoin as a method of payment.²¹

Since its 2011 inception, Silk Road has been the go-to black market for all sorts of illegal products and services. Its draw? The online marketplace offered an easy way to find goods and services -- and transact the money in secret. The site had 957,079 registered users, according to the FBI.

The site was operated on an anonymous network known as Tor, making activity on Silk Road virtually untraceable. The only money accepted on Silk Road was the digital currency bitcoin, adding an additional layer of anonymity to buyers and sellers.

The use of bitcoin helped Silk Road become a giant money laundering operation, according to the FBI. To process bitcoin transactions, Silk Road used what the FBI described as a "tumbler," a complex system that used countless dummy transactions to digitally conceal where the money came from. Over the past two and a half years, the FBI said the site generated revenue worth more than 9.5 million bitcoins -- valued at \$1.3 billion .²²

²¹ *The Bitcoin Protocol as Law, and the Politics of a Stateless Currency*, Sarah Jeong

²² <http://money.cnn.com/2013/10/02/technology/silk-road-shut-down/index.html?iid=EL>

Bitcoin markets “enable[] the easy laundering of funds”—“the act of transferring illegally obtained money through legitimate people or accounts so that its original source cannot be traced.” The Bitcoin community has developed “mixing services” that “can be used to mix one’s funds with others’, with the intention of confusing the trail [of Bitcoins] back to the original source. . . . Mixing helps protect privacy, but can also be used for money laundering.” One service, bitcoinfog.com, provides such a “mixing service” that prevents third parties from tracking Bitcoin transactions originating from a particular address; “if properly done[,] . . . you can eliminate any chance of finding your payments and making it impossible to prove any connection between a deposit and a withdraw[l] inside our service.” One quantitative analysis of Bitcoin transactions, compiled from data found in the public ledger, notes the “many strange looking changes and fork-merge structures, in which a large balance is either transferred within a few hours through hundreds of temporary intermediate accounts, or split into many small amounts which are sent to different accounts only in order to be recombined shortly afterwards.” Popular website Blockchain.info analyzes the amount of “tainted,” or known stolen, Bitcoins an identified address contains.²³

4. Legal Developments on Regulating the Bitcoin

²³ TRUST, IDENTITY, AND DISCLOSURE: ARE BITCOIN EXCHANGES THE NEXT VIRTUAL HAVENS FOR MONEY LAUNDERING AND TAX EVASION? ,*Sarah Gruber*

The use of Bitcoins poses many novel questions of law in a variety of legal areas. Courts will soon be faced with the need to apply the law to businesses that use Bitcoins or provide services to Bitcoin users.

On March 5, 2012, the now defunct Bitcoin exchange TradeHill filed suit against Dwolla, Inc., an online money transmitter service, for violation of the Racketeer Influenced and Corrupt Organizations Act (RICO), among various state law contract causes of action. The court dismissed the case pursuant to an arbitration clause contained in Dwolla's Terms of Use.

On May 2, 2013, a large US-based exchange, Coinlab, sued Mt. Gox in federal district court for an accounting, breach of contract, and breach of implied duty of good faith and fair dealing. Coinlab seeks damages in excess of \$75 million, despite the parties' contract providing for liquidated damages of only \$50 million in the event of breach of a particular provision.

On July 8, 2013, a group of plaintiffs filed a class action suit against BitInstant, alleging violations of the Electronic Funds Transfer Act, breach of contract, unjust enrichment, and negligence in connection with allegedly deceptive practices. It is clear that Bitcoin related disputes will become prevalent in the courts as the Bitcoin economy develops.

In 2013, the Securities and Exchange Commission issued an "investor alert to warn individual investors about fraudulent investment schemes that may involve Bitcoin and other virtual currencies."

In May of 2012, an FBI report entitled “Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity” was leaked to the Internet. The report, marked “Unclassified” yet “For Official Use Only,” revealed that “Bitcoin, like . . . other virtual currencies, provides opportunities for criminals to transfer, launder, or steal funds. . . . The way [the peer-to-peer system] creates, operates, and distributes Bitcoins makes it distinctively susceptible to illicit money transfers, and manipulation through the use of malware and botnets.

On May 14, 2013, the Department of Homeland Security seized a bank account owned by a company transacting with Dwolla and Mt. Gox upon probable cause that the contents of the account “were involved in transactions and attempted transactions in violation of 18 U.S.C. § 1960.” The supporting affidavit specifically alleges that the company “is engaged in a money transmitting business but is not registered as required with FinCEN..

In August 2013, Congress began an inquiry into the Bitcoin system when the Senate Homeland Security and Government Affairs Committee “sent letters to several agencies requesting that they disclose their virtual currency policies, how they developed them, how agencies are coordinating and finally what they plan to do going forward.²⁴

²⁴ TRUST, IDENTITY, AND DISCLOSURE: ARE BITCOIN EXCHANGES THE NEXT VIRTUAL HAVENS FOR MONEY LAUNDERING AND TAX EVASION?, *Sarah Gruber*

On August 2013, N.Y subpoenas Bitcoin firms in probe of criminal risk. New York's top banking regulator sent subpoenas to 22 digital-currency companies, including BitInstant LLC and Dwolla Corp., to determine whether new regulations should be adopted to govern the emerging industry, according to a person familiar with the matter.

"If virtual currencies remain a virtual Wild West for narco-traffickers and other criminals, that would not only threaten our country's national security, but also the very existence of the virtual currency industry as a legitimate business enterprise," said Benjamin Lawsky, superintendent of the state's Department of Financial Services, in a statement. DFS is "considering whether it should issue new regulatory guidelines specific to virtual currencies.". The subpoenas reflect the department's interest in more granular detail. According to his statement, Lawsky is concerned with consumer complaints regarding how quickly virtual currency transactions are processed.

The regulator, who threatened to pull the banking license of Standard Chartered Plc last August over violations of currency transfer sanctions against Iran, also expressed concern with criminal abuse of virtual currency markets.²⁵

²⁵ <http://www.bloomberg.com/news/2013-08-12/n-y-regulator-subpoenas-firms-over-bitcoin-crime-risks.html>

On August 5 2013 in SECURITIES AND EXCHANGE COMMISSION VS TRENDON T. SHAVERS and BITCOIN SAVINGS AND TRUST (see above), the defendant, Texan Trendon Shavers, was accused by the SEC of committing fraud in the form of a Bitcoin based Ponzi scheme²⁶ worth millions of dollars in today's Bitcoin market. But Shavers challenged the authority of the U.S. District Court where he was being tried, on the grounds that Bitcoins do not actually meet the definition of money, and therefore could not be the basis for a fraud charge.²⁷

4. Evaluation of the Bitcoin

i. Vulnerabilities of the Bitcoin

Uncertainty

Despite the potential advantages of digital currencies like Bitcoin, their wide-spread adoption faces a number of obstacles. First and foremost, economists are worried about the uncertainty surrounding the

²⁶ <http://www.nbcnews.com/business/sec-says-texas-man-ran-bitcoin-ponzi-scheme-6C10722287>

²⁷ Bitcoin is a currency': Federal judge says the virtual cash is real money Devin Coldewey NBC News, <http://www.nbcnews.com/technology/bitcoin-currency-federal-judge-says-virtual-cash-real-money-6C10874611>

operation and growth of digital currencies. Because so much of the data on these currencies is either supplied directly by the issuer or scattered across the Internet, it is difficult for scholars to draw any reliable conclusions on whether—and if so, how and when—these currencies might be widely accepted. Others criticize digital currencies like Bitcoin on a more theoretical level because they are neither intrinsically valuable, like gold, nor do they have roots in a commodity expressing a certain purchasing power. Some critics go as far as to describe digital currencies like Bitcoin as nothing more than a Ponzi scheme.

Lack of regulation

The lack of an underlying legal framework poses additional problems. Because digital currencies like Bitcoin lack regulation or public oversight, they are subject to credit, liquidity, and operational risks, as well as risk of fraud. The lack of oversight coupled with the finality and irrevocability of Bitcoin transactions gives many skeptics cause for concern. Because digital currency transactions necessarily occur over the Internet, cybersecurity is a constant concern. Despite the technical measures used to secure individual Bitcoin transactions, user-end storage and usage of Bitcoins are a key security vulnerability. For instance, in June 2011, a hacker compromised a user account containing about 400,000 Bitcoins, totaling approximately \$9 million, causing the value of one Bitcoin to plummet from \$17.50 to \$0.01 in only a few hours.

Network Externalities

Finally, digital currencies like Bitcoin face the problem of network externalities. The benefit of using a digital currency depends on the number of other users: if few merchants accept digital money, the benefits to households to use digital money products are low; if few consumers use digital money, a merchant has little incentive to accept digital cash. Thus, even if digital currencies are able to overcome the aforementioned barriers, their biggest challenge lies in convincing users to use them and merchants to accept them.²⁸

ii. Security incidents

From time to time, Bitcoin is surrounded by controversy. Sometimes it is linked to its potential for becoming a suitable monetary alternative for drug dealing and money laundering, as a result of the high degree of anonymity.

On other occasions, users have claimed to have suffered a substantial theft of Bitcoins through a Trojan that gained

²⁸ REGULATING DIGITAL CURRENCIES: BRINGING BITCOIN WITHIN THE REACH OF THE IMF
, Nicholas A. Plassaras

access to their computer. The Electronic Frontier Foundation, which is an organization that seeks to defend freedom in the digital world, decided not to accept donations in Bitcoins anymore. Among the reasons given, they considered that “Bitcoin raises untested legal concerns related to securities law, the Stamp Payment Act, tax evasion, consumer protection and money laundering, among others”.

However, practically identical problems can also occur when using cash, thus Bitcoin can be considered to be another variety of cash, i.e. digital cash. Cash can be used for drug dealing and money laundering too; cash can also be stolen, not from a digital wallet, but from a physical one; and cash can also be used for tax evasion purposes. The question is not so much related to the format of money as such (physical or digital), but rather to the use people make of it. Nevertheless, if the use of digital money in itself complicates investigations and law enforcement, special requirements may be needed. Therefore, the real dimension of all these controversies still needs to be further analyzed. Bitcoin has also featured in the news, in particular following a cyberattack perpetrated on 20 June 2011, which managed to knock the value of the currency down from USD 17.50 to USD 0.01 within minutes. Apparently, around 400,000 Bitcoins (worth almost USD 9 million) were involved. According to currency exchange Mt.Gox, one account with a lot of Bitcoins was compromised and whoever stole it (using a Hong Kong based IP to login) first sold all the Bitcoins in there, only to buy them back again immediately afterwards, with the intention of withdrawing the coins. The USD 1,000/day withdrawal limit was active for this account and the hacker was only able to exchange USD 1,000 worth of Bitcoins.

Apart from this, no other accounts were compromised, and nothing was lost. The evolution of Bitcoin's exchange rate on the Mt.Gox exchange platform during the hours of the incident, and is also the expression of how an immature and illiquid currency can almost completely disappear within minutes, causing panic to thousands of users. In addition, the perpetrator hacked into the Mt.Gox database, gaining access to usernames, e-mail addresses and hashed passwords for thousands of users. Mt.Gox reacted by closing the system for a few days and by promising that the transactions carried out by the hacker would be reversed.

Bitcoin defenders claim that the Bitcoin system did not fail. The problem was related to a particular trading platform– Mt.Gox– which did not have strong enough security measures. In a more recent case (May 2012), the exchange platform Bitcoinica lost 18,547 Bitcoins from its deposits following a cyber attack, in which sensitive customer data might also have been obtained.

Another recurrent issue is whether Bitcoin works like a Ponzi scheme or not. Users go into the system by buying Bitcoins against real currencies, but can only leave and retrieve their funds if other users want to buy their Bitcoins, i.e. if new participants want to join the system. For many people, this is characteristic of a Ponzi scheme. The US Securities and Exchange Commission defines a Ponzi scheme in the following terms:

A Ponzi scheme is an investment fraud that involves the payment of purported returns to existing Investors from funds contributed by new investors. Ponzi scheme organizers often solicit new investors by promising to invest funds in opportunities claimed to generate high returns with little or no risk. In many Ponzi schemes, the fraudsters focus on attracting new money to make promised payments to earlier-stage investors and to use for personal expenses, instead of engaging in any legitimate investment activity.

On the one hand, the Bitcoin scheme is a decentralized system where – at least in theory – there is no central organizer that can undermine the system and disappear with its funds.

Bitcoin users buy and sell the currency among themselves without any kind of intermediation and therefore, it seems that nobody benefits from the system, apart from those who benefit from the exchange rate evolution (just as in any other currency trade) or those who are hard-working “miners” and are therefore rewarded for their contribution to the security and confidence in the system as a whole.

Moreover, the scheme does not promise high returns to anybody. Although some Bitcoin users may try to profit from exchange rate fluctuations, Bitcoins are not intended to be an investment vehicle, just a medium of exchange. On the contrary, Gavin Andresen, Lead Developer of the Bitcoin virtual currency project, does not hesitate to say that “Bitcoin is an

experiment. Treat it like you would treat a promising internet start-up company: maybe it will change the world, but realize that investing your money or time in new ideas is always risky". In addition, Bitcoin supporters claim that it is an open-source system whose code is available to any interested party.

However, it is also true that the system demonstrates a clear case of information asymmetry. It is complex and therefore not easy for all potential users to understand. At the same time, however, users can easily download the application and start using it even if they do not actually know how the system works and which risks they are actually taking. This fact, in a context where there is clear legal uncertainty and lack of close oversight, leads to a high-risk situation. Therefore, although the current knowledge base does not make it easy to assess whether or not the Bitcoin system actually works like a pyramid or Ponzi scheme, it can justifiably be stated that Bitcoin is a high-risk system for its users from a financial perspective, and that it could collapse if people try to get out of the system and are not able to do so because of its illiquidity. The fact that the founder of Bitcoin uses a pseudonym – Satoshi Nakamoto – and is surrounded by mystery does nothing to help promote transparency and credibility in the scheme.

All these issues raise serious concerns regarding the legal status and security of the system, as well as the finality and irrevocability of the transactions, in a system which is not subject to any kind of public oversight. In June 2011 two US senators, Charles Schumer and Joe Manchin, wrote to the Attorney General and to the Administrator of the Drug Enforcement

Administration expressing their worries about Bitcoin and its use for illegal purposes. Mr Andresen was also asked to give a presentation to the CIA about this virtual currency scheme.¹⁶ Further action from other authorities can reasonably be expected in the near future.²⁹

iii. Bitcoin and Price Stability

ECB in “VIRTUAL CURRENCY SCHEMES”, concluded on bitcoin posing risk to the price stability “While subject to a lack of reliable information, we can conclude that virtual currency schemes do not pose a risk for price stability at this stage, provided that the issuance of money continues to be as stable as it seems to be at present. In the short to medium term, no significant impact can be expected on the velocity of money. However, it is probably worth monitoring the interaction between virtual currencies and the real world.”

On December 2013, China’s central bank barred financial institutions from handling Bitcoin transactions, moving to regulate the virtual currency after an 89-fold jump in its value sparked a surge of investor interest in the country. Bitcoin plunged more than 20 percent to below \$1,000 on the Bitstamp Internet exchange after the People’s Bank of China said it isn’t a currency with “real meaning” and doesn’t have the same legal status. The public

²⁹ European Central Bank: VIRTUAL CURRENCY SCHEMES

is free to participate in Internet transactions provided they take on the risk themselves, it said. The ban reflects concern about the risk the digital currency may pose to China's capital controls and financial stability after a surge in trading this year made the country the world's biggest trader of Bitcoin, according to exchange operator BTC China. Bitcoin's price jumped more than ninefold in the past two months alone, prompting former Federal Reserve Chairman Alan Greenspan to call it a "bubble."³⁰

Iv .The Need for Regulation

The instability of virtual currency schemes can be explained by one of the most critical aspects i.e. the lack of a proper legal basis for virtual currency schemes. The legal basis of a payment system consists of framework legislation, as well as specific laws, regulations, and agreements governing both payments and the operation of the system. Virtual currency schemes visibly lack a proper legal framework, as well as a clear definition of rights and obligations for the different parties. Key payment system concepts such as the finality of the settlement do not seem to be clearly specified.

Furthermore, the global scope that most of these virtual communities enjoy not only hinders the Identification of the jurisdiction under which the system's rules and procedures should eventually be interpreted, it also means the location of the participants and the scheme owner are hard to establish. As a consequence, governments and central banks would face serious

³⁰ <http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html>

difficulties, if they tried to control or ban any virtual currency scheme, and it is not even clear to what extent they are permitted to obtain information from them. In the particular case of Bitcoin, which is a decentralized peer-to-peer virtual currency scheme, there is not even a central point of access, i.e. there is no server that could be shut down if the authorities deemed it necessary.³¹

The non-existence of a clear legal basis for virtual currency schemes is an illustration of the overall existing lack of understanding about virtual economies and their impact on the real economy. For instance, it is not clear to what extent virtual production should be considered when estimating the production of wealth per capita. The current national income and product accounts do not assign any value to online assets (see Castronova, 2001). Moreover, two related aspects that could be considered are how to tax individual income earned through virtual currency transactions and how to define and protect virtual properties³².

PBOC, China Banking Regulatory Commission and other regulators have held discussions about drafting rules for trading platforms that facilitate the buying and selling of the virtual money, two people with direct

³¹ European Central Bank : Virtual Currency Schemes

³² see **Chu, 2008 and The Economist, 2011b**, ³² European Central Bank : Virtual Currency Schemes

knowledge of the matter said. They were not authorized to speak because the information is not public. "We're happy to see the government start regulating the Bitcoin exchanges," Chief Executive Officer Bobby Lee of BTC China, the largest Bitcoin exchange in the country, said in a phone interview before the PBOC announcement. Regulations would be for "the good of the consumer," he said. BTC is seeking recognition of the currency so it can be used to buy goods and services instead of being used for speculation, he said.³³

FinCEN is the only US federal regulator to have released official guidance on the use of Bitcoin. In March 2013, FinCEN published interpretive guidance clarifying the application of the Bank Secrecy Act and the USA PATRIOT Act to Bitcoin and other convertible digital assets by stating that any administrator or exchanger of bitcoins (or other convertible digital asset) must be a registered MSB under FinCEN's money transmitter regulations. The release indicated that individual users of bitcoins that are not operating a business would not be considered MSBs and therefore would not be required to register, report or perform recordkeeping. Such clarification also requires administrators or exchangers of bitcoins to comply with applicable state law and register with certain state regulatory agencies.

Furthermore, various state regulators, including the California Department of Financial Institutions, the Idaho Department of Financial Services and the New York Department of Financial Services, have

³³ <http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html>

followed FinCEN's example and have issued interpretations or mandates requiring that Bitcoin exchanges and service providers register and/or seek licenses on a state level as money transmitters or MSB.³⁴

A Justice Department official said Nov. 18 Bitcoins can be “legal means of exchange” at a U.S. Senate committee hearing, boosting prospects for wider acceptance of the virtual currency. Fed Chairman Ben S. Bernanke told the Senate committee the U.S. central bank has no plans to regulate the currency.³⁵

The Bank of France warned on Thursday about risks related to the digital currency bitcoin, adding its voice to growing concerns about the unregulated, online money. Bitcoin is not backed by any central bank or government, or by physical assets. Their value depends on people's confidence in the currency. It has been gaining acceptance by the general public and investment community but have yet to become an accepted form of payment on websites of major retailers such as Amazon.com. The Bank of France said the price of bitcoin in legal currencies was inherently volatile and users may find it difficult to convert to real money. The anonymity that bitcoin offer users also raises the risk that they could also be used for money-laundering and financing of terrorism, the central bank said in a publication.

³⁴ Article by [Katten Muchin Rosenman's Corporate Practice Group](#) and [Katten Muchin Rosenman LLP's Financial Services Practice Group](#) Katten Muchin Rosenman LLP

³⁵ <http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html>

"Even if bitcoin is not currently a credible investment vehicle and therefore do not pose a significant risk to financial stability, they represent a financial risk for those who hold them," the Bank of France said and warned that speculating on the price of bitcoin could become costly if other users became unwilling to convert gains into legal tender, potentially putting the whole system at risk of collapse if bitcoin demand evaporated. Noting a growing number of retailers and service providers who accept bitcoin for payment in France, the central bank warned they benefited from no guarantee that the bitcoin could be cashed for real money.³⁶

Regardless of which measure is chosen, the potential need for a method to combat speculative attacks using Bitcoin is clear. As the Internet continues to play an increasingly important role in how we conduct commerce, our institutions have to adjust to the new challenges this change creates. The evolution of Bitcoin is no exception. Although still in its nascent stages, Bitcoin and other digital currencies like it are projected to become important players in the future of e-commerce. The time to consider how to prepare for that future is now, before practical problems arise.³⁷

³⁶ <http://www.reuters.com/article/2013/12/05/us-france-bitcoin-idUSBRE9B40IF20131205>

³⁷ REGULATING DIGITAL CURRENCIES: BRINGING BITCOIN WITHIN THE REACH OF THE IMF ,Nicholas A. Plassaras

INTERNATIONAL HELLENIC UNIVERSITY

LL.M IN TRANSNATIONAL AND EUROPEAN COMMERCIAL LAW & ALTERNATIVE DISPUTE
RESOLUTION